



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/635,778	08/11/2000	David M. Goldschlag	2685/5681	1089

7590 10/31/2005
WENDY E. KOBÄ, ESQ
P.O. BOX 556
SPRINGTOWN,, PA 18081-0556

EXAMINER

MYHRE, JAMES W

ART UNIT	PAPER NUMBER
----------	--------------

3622

DATE MAILED: 10/31/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/635,778

Applicant(s)

GOLDSCHLAG ET AL

Examiner

James W. Myhre

Art Unit

3622

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 27 September 2005.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 13-27 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 13-27 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Amendment

1. The amendment filed on September 27, 2005 is sufficient to overcome the previous rejection by canceling Claims 1-12. The currently pending claims considered below are Claims 13-27.

Claim Rejections - 35 USC § 101

2. The amendment filed on September 27, 2005 canceled Claims 1-12 that were rejected under 35 U.S.C. 101 in paragraph 3 of the June 27, 2005 Office Action. Therefore, the Examiner hereby withdraws that rejection.

Allowable Subject Matter

3. The indicated allowability of claims 13-27 is withdrawn in view of the new interpretation of the claimed subject matter. Rejections based on the new interpretation follow.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the

Art Unit: 3622

applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 13-27 are rejected under 35 U.S.C. 102(e) as being anticipated by

Challener et al (6,081,793).

Claims 13, 15, 17, 21-24: Challener discloses a system, apparatus, and program for electronic voting, comprising:

- a. a processor (Item 55, Figure 2b);
- b. instructions to cause the processor to perform the steps of:
 - (1) receiving a voter registration request message (ballot request) that will bind vote authorization data (voter identification and PIN) and a blinded unvalidated vote certificate (ballot)(col 6, line 65 – col 7, line 4);
 - (2) determine if the vote authorization data is valid (col 7, lines 4-16);
 - (3) validating the blinded unvalidated vote certificate to obtain a blinded vote certificate if the vote authorization data is valid (col 7, lines 4-16); and
 - (4) sending a response message to the voter that includes the blinded validated vote certificate (certified ballot) atomically bound to the voter registration request message (col 7, lines 4-16); and
- c. memory coupled to the processor (col 3, lines 30-35).

The Examiner notes that Challener discloses that the user receives a smart card when registering to vote. The smart card contains the voter identification, public encryption key, a ballot box ID, and a PIN number for the voter (i.e. vote authorization data). On election day, the voter places his smart card in a smart card reader of the authentication server at the polling station and enters his PIN number to validate his identity which generates a "ballot request". The Examiner considers the entering of the smart card information and the PIN number and the resultant ballot request to be the equivalent of the claimed voter registration request message. The authentication server uses the PIN number to determine if the smart card information (vote authorization data) is valid. If the vote authorization data is valid, the polling station selects a ballot ID, encrypts it along with the voter authorization data and "sends the encrypted ballot, and the ballot ID, to the voter's personal computer" (col 8, lines 1-9). The voter then decrypts the ballot with the smart card encryption key, enters his selections onto the ballot, re-encrypts the ballot using the smart card encryption key, and returns the encrypted ballot to the voting system. The system uses at least two servers, each able to decrypt only a portion of the encrypted ballot to maintain the anonymity of the voter, while also allowing for the verification of the vote, if necessary. Thus, Challener uses blinded encryption methods. The Examiner considers the initial ballot selected by the polling station to be the equivalent of the claimed blinded unvalidated voter certificate; the encrypted ballot sent to the voter's personal computer as the blinded validated voter certificate.

Claims 14, 16, and 18: Challenger discloses an apparatus for electronic voting as in Claims 13, 15, and 17 above, and further inherently discloses the certificate indicating a yes or no vote (col 1, lines 11-15). The Examiner notes that ballots contain one or more questions to which the voter may make one or more selections based on his desires. Each of these selections is a vote for or against the topic of the question – whether it is a “for” (yes) or “against” (no) vote on a local tax levy proposition, “for” (yes) or “against” (no) the Presidential candidates, or “for” (yes) or “against” (no) several candidates running for several open councilmen positions. In each case, the completed ballot indicates the voter’s yes or no votes.

Claim 19: Challenger discloses an apparatus for electronic voting, comprising:

- a. a processor (Item 55, Figure 2b);
- b. instructions to cause the processor to perform the steps of:
 - (1) receiving a voter registration request message (ballot request) that will bind vote authorization data (voter identification and PIN) and a blinded unvalidated vote certificate (ballot)(col 6, line 65 – col 7, line 4);
 - (2) determine if the vote authorization data is valid (col 7, lines 4-16);
 - (3) validating the blinded unvalidated vote certificate to obtain a blinded vote certificate if the vote authorization data is valid (col 7, lines 4-16); and

- (4) sending a response message to the voter that includes the blinded validated vote certificate (certified ballot) atomically bound to the voter registration request message (col 7, lines 4-16); and
- c. memory coupled to the processor (col 3, lines 30-35).

The Examiner notes that Challener discloses that the user receives a smart card when registering to vote. The smart card contains the voter identification, public encryption key, a ballot box ID, and a PIN number for the voter (i.e. vote authorization data). On election day, the voter places his smart card in a smart card reader of the authentication server at the polling station and enters his PIN number to validate his identity which generates a "ballot request". The Examiner considers the entering of the smart card information and the PIN number and the resultant ballot request to be the equivalent of the claimed voter registration request message. The authentication server uses the PIN number to determine if the smart card information (vote authorization data) is valid. If the vote authorization data is valid, the polling station selects a ballot ID, encrypts it along with the voter authorization data and "sends the encrypted ballot, and the ballot ID, to the voter's personal computer" (col 8, lines 1-9). The voter then decrypts the ballot with the smart card encryption key, enters his selections onto the ballot, re-encrypts the ballot using the smart card encryption key, and returns the encrypted ballot to the voting system. The system uses at least two servers, each able to decrypt only a portion of the encrypted ballot to maintain the anonymity of the voter, while also allowing for the verification of the vote, if necessary. Thus, Challener uses blinded encryption methods. The Examiner considers the initial ballot selected by the

Art Unit: 3622

polling station to be the equivalent of the claimed blinded unvalidated voter certificate; the encrypted ballot sent to the voter's personal computer as the blinded validated voter certificate.

Challenger also discloses methods to tabulate, correct, or challenge the votes through the use of a journal server which keeps track of each vote as it is being entered. To correct a vote, the voter again enters his PIN number and smart card data (which includes the validated ballot)(i.e. "receives a second voting transaction message)", the system revalidates the voter (ballot)(i.e. "determines if the second voting transaction message has the same nonce, session key, and blinding factor" as the previous stored ballot); and retrieves the previously stored ballot if the second request message is valid (col 10, line 51 – col 11, line 37).

Claim 20: Challenger discloses an apparatus for electronic voting as in Claim 19 above, and further inherently discloses the certificate indicating a yes or no vote (col 1, lines 11-15). The Examiner notes that ballots contain one or more questions to which the voter may make one or more selections based on his desires. Each of these selections is a vote for or against the topic of the question – whether it is a "for" (yes) or "against" (no) vote on a local tax levy proposition, "for" (yes) or "against" (no) the Presidential candidates, or "for" (yes) or "against" (no) several candidates running for several open councilmen positions. In each case, the completed ballot indicates the voter's yes or no votes.

Art Unit: 3622

Claims 25-27: Challenger discloses a system for electronic voting as in Claim 24 above, and further discloses means for auditing, initializing, and recovering from an interruption in an electronic voting transaction (col 10, line 51 – col 11, line 37).

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Exr. James W. Myhre whose telephone number is (571) 272-6722. The examiner can normally be reached Monday through Thursday from 5:30 a.m. to 3:30 p.m.

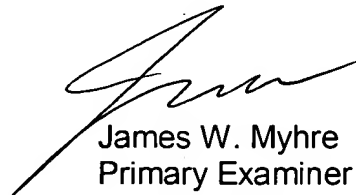
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Eric Stamber, can be reached on (571) 272-6724. The fax phone number for Formal or Official faxes to Technology Center 3600 is (571) 273-8300. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 273-6722.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-3600.



JWM

October 27, 2005



James W. Myhre
Primary Examiner
Art Unit 3622